Improving e-payment security using Elliptic Curve Cryptosystem.

Department of Computer Science, University of Agriculture, PMB 2240, Abeokuta, Ogun State, Nigeria

Abstract

The use of e-commerce has been associated with a lot of skepticism and apprehension due to some crimes associated with e-commerce and specifically to payment systems. The secure socket layer (SSL) protocol is trusted in this regard to secure transactions for sensitive applications like e-commerce. Unfortunately, the use of SSL protocol causes slow response time on the server which is a major cause of frustration for on-line shoppers. In this paper, we propose a secured credit-debit card payment systems based on Elliptic Curve Cryptosystem (ECC). We first examined ECC algorithm over prime fields $GF(p)$, implement our proposed method using a typical transaction involving credit/debit card numbers and compared the performance with RSA cryptosystem. Our result shows that ECC is faster in terms of response to transaction request and occupies less memory space than equivalent RSA system. Thus, these makes it more suitable public Key cryptography scheme for application in a constraint open environment like payment system where fast operations are needed.